·安全技术· 文章编号：1000-3428(2016)04-0137-06 文献标识码：A 中图分类号：TP309

适用于空间 DTN 的非交互式密钥交换协议

杜瑞颖[1a,1b]，周振玉[1a,1b]，米兰·黑娜亚提[2]

（1. 武汉大学 a. 计算机学院；b. 空天信息安全与可信计算教育部重点实验室，武汉 430072；
2. 新疆广播电视大学远程教育学院，乌鲁木齐 830049）

摘 要： 针对空间时延容忍网络高延时、连接易中断等特点，提出一种非交互式的密钥交换协议，并在随机预言模型下对其进行安全性证明。该协议无需用户交互即生成一个共享的对称密钥，可消除对传统公钥基础设施中证书的依赖，减少通信与存储开销，同时避免基于身份的公钥加密体制中存在的密钥托管问题。分析结果表明，该协议未使用耗时的双线性对运算，具有较高的计算效率，更适用于计算能力受限、能量资源宝贵的空间环境。

关键词： 时延容忍网络；非交互式密钥交换；无证书密码；可证明安全；随机预言模型

中文引用格式： 杜瑞颖，周振玉，米兰·黑娜亚提. 适用于空间 DTN 的非交互式密钥交换协议[J]. 计算机工程，2016，42(4)：137-142.

英文引用格式： Du Ruiying，Zhou Zhenyu，Milan Heinayati. Non-interactive Key Exchange Protocol for Space DTN[J]. Computer Engineering，2016，42(4)：137-142.

Non-interactive Key Exchange Protocol for Space DTN

DU Ruiying[1a,1b]，ZHOU Zhenyu[1a,1b]，Milan Heinayati[2]

（1a. School of Computer；1b. Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education，Wuhan University，Wuhan 430072，China；2. Distance Learning College，Xinjiang Radio and TV University，Urumqi 830049，China）

【Abstract】 The space Delay Tolerant Network（DTN）has characteristic such as high delay and frequent disconnectivity. Aiming at this problem，this paper designs a non-interactive key exchange protocol，and it is proven secure in the random oracle model. The proposed protocol enables two parties to agree on a symmetric shared key without requiring any interaction. The protocol eliminates the dependency on certificate used in Public Key Infrastructure（PKI）and avoids the key escrow problem in ID-based Public Key Cryptography（ID-PKC）. Analysis result shows that the proposed protocol does not utilize the expensive pairing computation and achieves higher efficiency compared with other Non-interactive Key Exchange（NIKE）protocols，and thus proves to be suitable for the space environment with restricted computing and few power resource.

【Key words】 Delay Tolerant Network（DTN）；non-interactive key exchange；certificateless cryptography；provable security；random oracle model

DOI： 10.3969/j.issn.1000-3428.2016.04.025

1 概述

时延容忍网络（Delay Tolerant Network，DTN）是一种位于区域网络之上的覆盖网，用以克服受限网络环境下频繁的网络断开、高延迟和异构性等问题。随着深空探测、星际网络等领域研究的发展，空间 DTN 越来越受到关注，然而该网络环境具有传播时延大、链路不对称和连接易中断等缺点，终端节点的能量和计算能力有限。因此，传统网络的安全协议和机制对这种网络并不适用[1]。

在传统网络中，研究者广泛使用公钥基础设施（Public Key Infrastructure，PKI）来保证数据的机密性和完整性，然而这需要大量的证书合法性验证和证书撤销列表检查操作，对网络连接可用性以及带宽有很高的要求，显然这在 DTN 环境中是无法满足的。为了保证空间 DTN 网络中数据的机密性和完整性，IRTF 的 DTN 研究小组（DTNRG）发布了一个安全协议规范 BSP[2]，提供了 4 种网络层上的安全服务，但这并未完全解决 DTN 空间网络中的密钥管理问题。文献[3]利用基于身份的非交互式密钥协

基金项目： 国家自然科学基金资助项目“无线 Mesh 网络中跨层安全关键技术研究”（61272451）。

作者简介： 杜瑞颖（1964－），女，教授、博士，主研方向为网络安全；周振玉、米兰·黑娜亚提，硕士。

收稿日期： 2015-04-03 **修回日期：** 2015-05-03 **E-mail：** 962417506@qq.com

商方案提出了适用于 DTN 的匿名通信协议(ID-NIKE),其具有无需用户交互的优点,但是由于使用了基于身份的密码,存在固有的密钥托管问题。文献[1,4]探讨了利用双信道加密和带外传输来传递公钥,为 DTN 的安全通信提供前提保障,但并未涉及如何协商对称密钥。文献[5-6]设计了适用于卫星网络的密钥协商协议,但采用的是交互式协商方式,对延迟较大的空间 DTN 并不适用。

保证安全通信最基本的方法是使用对称密钥对传输数据进行加密,本文主要关注如何在空间 DTN 环境中产生用于安全通信的对称密钥。对称密钥通常可由密钥协商协议产生,现有密钥协商方案为具有各种安全属性,多数设计为基于交互式的,例如被广泛使用的 SSL 和 TLS 协议,但是这类协议需要通信双方一轮或多轮的交互,耗费大量时间的同时也消耗大量带宽和能量,因此在空间 DTN 网络中并不适用。文献[7-9]提出了非交互式的密钥交换(Non-interactive Key Exchange NIKE)协议,该协议可以令通信双方在不需要任何交互的情况下,仅利用自己私有的信息和对方公开的信息,计算产生一个双方共享的对称密钥。NIKE 具有节省通信量和带宽、低能耗[10]等优点,但是,目前大部分 NIKE 方案都是基于 PKI 或基于 ID,根据上文分析,PKI 并不适合空间 DTN 网络,基于身份密码则存在密钥托管问题,在非交互式的密钥协商中,私钥生成中心(Private Key Generator,PKG)总是能够计算出用户间共享的对称密钥,造成一定的安全隐患,而且基于身份的公钥加密体制(ID-based Public Key Cryptography, ID-PKC)需要在 PKG 和用户之间建立安全信道来传递 PKG 生成的私钥。

本文在已有研究的基础上,提出一种适用于空间 DTN 的非交互式密钥交换协议,使 DTN 节点在不需要交互的情况下,协商出会话密钥。

2 预备知识

2.1 非交互式密钥协商定义

NIKE 方案包含 3 个算法:系统初始化(*Setup*),用户公私钥对生成算法(*NIKE. KeyGen*)和用户共享密钥生成算法(*SharedKey*)。本文的 NIKE 是定义在无证书密码环境下的,用户的私钥由用户选取的秘密值和密钥生成中心(Key Generator Center, KGC)产生的部分私钥共同计算产生。

(1)*Setup* 算法:

$(msk, params) \leftarrow Setup(1^k)$

输入安全参数 k,输出系统公共参数 *params* 和系统主密钥 *msk*,其中,*params* 公开,*msk* 保密。

(2)*NIKE. KeyGen* 算法:

$(pk_{ID}, sk_{ID}) \leftarrow NIKE.\ Keygen(params, msk, ID, z)$

输入系统公共参数 *params*、系统主密钥 *msk*、用户身份 *ID*、用户选取的秘密值 z,输出用户的公私钥对 (pk_{ID}, sk_{ID})。

(3)*SharedKey* 算法:

$K_{A,B} \leftarrow Sharedkey(params, ID_A, SK_A, ID_B, PK_B, j)$

由用户执行,输入系统公共参数 *params*、用户 A 和用户 B 的身份 *ID*、用户 A 的私钥 SK_A 和用户 B 的公钥 PK_B(用户 B 使用自己的私钥 SK_B 和用户 A 的公钥 PK_A),j 为时间戳或密钥协商次数,输出共享对称密钥 $K_{A,B}$。

NIKE 要求双方用户计算共享密钥时使用的算法相同,且给定任意 2 个用户 ID_A,ID_B 对应公私钥对 (PK_A, SK_A),(PK_B, SK_B),满足一致性要求:

$$SharedKey(params, ID_A, SK_A, ID_B, PK_B, j) = SharedKey(params, ID_B, SK_B, ID_A, PK_A, j)$$

2.2 无证书公钥体制

为解决 ID-PKC 中存在的的密钥托管问题,文献[11]提出了无证书公钥加密体制(Certificateless PKC,CL-PKC),CL-PKC 同时也消除了传统 PKI 中对证书的使用。在 CL-PKC 中,由于用户的私钥是由 KGC 和用户共同生成的,因此 KGC 不知道用户的完整私钥,即使 KGC 被敌手攻陷也会在一定程度上保护用户的秘密通信。CL-PKC 的提出解决了 ID-PKC 的密钥托管问题,同时相比传统 PKI 体制减小了成本和开销。目前,已有许多基于无证书的加密、签名、密钥协商方案被提出。

2.3 困难假设

本文提出的协议安全性依赖于 CDH 困难假设(Computational Diffie-Hellman assumption,CDH):令 p,q 为 2 个大素数,且满足 $q \mid p-1$,令 g 是 Z_q^* 的一个 q 阶生成元,给定一个元组 (g, g^a, g^b),其中,$a, b \in Z_q^*$ 是未知的,要计算 $g^{ab} \bmod p$ 是困难的。

3 本文协议

3.1 系统模型

空间 DTN 本质是一种存储-运载-转发网络,数据存储在 DTN 设备的永久存储体中,当链接可用时再转发至其他节点。在 DTN 体系结构中,主要有 3 个组成部分:节点,网关和路由。路由主要在同种网络中工作,网关负责不同网络之间的传输。在下文描述中,空间 DTN 各类通信节点和终端统称为用户。空间 DTN 系统模型如图 1 所示[12]。

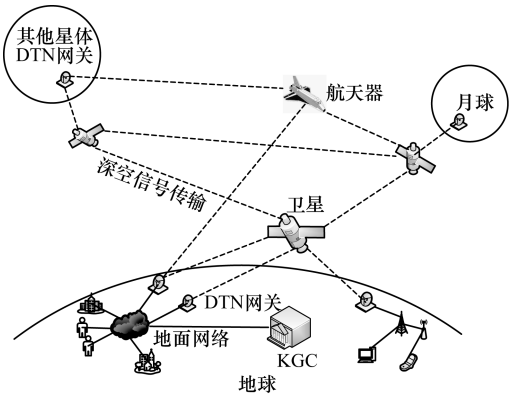

图 1　空间 DTN 系统模型

3.2　非交互式密钥交换协议

本文协议流程如图 2 所示,其中主要包含 3 个阶段:系统初始化,用户注册和共享密钥生成。为了方便描述,空间 DTN 环境中的航天器、卫星等通信节点在协议中都统称为“用户”。系统初始化用于生成系统公共参数、系统主密钥以及系统公钥;用户注册阶段即用户密钥生成阶段,完成注册的合法用户会获得保密私钥和公开的公钥;在获得对方的公钥后,用户利用共享密钥生成算法来生成共享的对称会话密钥,进而进行安全通信。

系统建立	系统主密钥$msk=x$，系统公钥$mpk=g^x$，公共参数$params$	
生成用户公私钥对	用户A $PK_A=(\mu_A,\omega_A)$ $SK_A=(z_A,d_A)=(z_A,s_A+xH_1(ID_A,\mu_A,\omega_A))$	用户B $PK_B=(\mu_B,\omega_B)$ $SK_B=(z_B,d_B)=(z_B,s_B+xH_1(ID_B,\mu_B,\omega_B))$
生成用户共享密钥	$K_A=(\mu_B{}^{h_{A,B}}\omega_B y^{Q_B})^{h_{B,A}z_A+d_A}$ $K_{A,B}=\begin{cases}H_3(ID_A,\mu_A,\omega_A,ID_B,\mu_B,\omega_B,K_A,j) & ID_A<ID_B\\ H_3(ID_B,\mu_B,\omega_B,ID_A,\mu_A,\omega_A,K_A,j) & ID_A<ID_B\end{cases}$	$K_B=(\mu_A{}^{h_{B,A}}\omega_A y^{Q_A})^{h_{A,B}z_B+d_B}$ $K_{B,A}=\begin{cases}H_3(ID_A,\mu_A,\omega_A,ID_B,\mu_B,\omega_B,K_B,j) & ID_A<ID_B\\ H_3(ID_B,\mu_B,\omega_B,ID_A,\mu_A,\omega_A,K_B,j) & ID_A<ID_B\end{cases}$

图 2　本文协议过程

具体步骤如下:

(1) 系统建立

系统初始化阶段,输入安全参数 k,生成 2 个大素数 p 和 q,$p=2q+1$,其中,q 的长度为 k;g 是 Z_q^* 的一个阶为 q 的生成元。随机选择 $x\in Z_q^*$,计算 $y=g^x \bmod p$作为 KGC 的系统公钥。

选择 Hash 函数 $H_1\sim H_3$。

$H_1:\{0,1\}^* \times Z_p^* \times Z_p^* \rightarrow Z_q^*$

$H_2:\{0,1\}^* \rightarrow Z_q^*$

$H_3:\{0,1\}^* \rightarrow Z_q^*$

公布系统公共参数 $params=\{p,q,g,y,H_1,H_2,H_3\}$,系统主密钥 $msk=x$,系统公钥 $mpk=g^x$。

(2) 密钥提取

用户注册阶段,用户获得保密的私钥并公开自己的身份信息和公钥。

1)用户身份为 ID,用户随机选择 $z_{ID}\in Z_q^*$,计算 $\mu_{ID}=g^{z_{ID}} \bmod p$,将$\mu_{ID}$发送给 KGC。

2)KGC 接收到 ID 和 μ_{ID}后,随机选择 $s_{ID}\in Z_q^*$,计算:

$$\omega_{ID}=g^{s_{ID}} \bmod p$$

$$d_{ID}=s_{ID}+xH_1(ID,\omega_{ID},\mu_{ID}) \bmod q$$

然后将(ω_{ID},d_{ID})发送给用户。

3)用户收到(ω_{ID},d_{ID})后,验证部分私钥 d_{ID}的合法性以及 $g^{d_{ID}}=\omega_{ID}y^{H_1(ID,\omega_{ID},\mu_{ID})}$ 是否成立,若等式成立则接收(ω_{ID},d_{ID}),否则拒绝。

4)设置私钥 $SK_{ID}=(z_{ID},d_{ID})$,公钥 $PK_{ID}=(\mu_{ID},\omega_{ID})$。

(3) 共享密钥计算

用户 A 公私钥对为(PK_A,SK_A),用户 B 公私钥对为(PK_B,SK_B)。

1)用户 A 计算:

$$K_A=(\mu_B h_{A,B}\omega_B y^{Q_B})^{h_{B,A}z_A+d_A}$$

其中,$h_{A,B}=H_2(ID_A,\mu_A,\omega_A,ID_B,\mu_B,\omega_B,j)$,$j$ 起到时间戳的作用,可以理解为 A 和 B 第 j 次计算共享密钥;$Q_{ID}=H_1(ID,\omega_A,\mu_A)$。然后计算共享密钥,这里假设 ID 自然有序,有:

$$K_{A,B}=\begin{cases}H_3(ID_A,\mu_A,\omega_A,ID_B,\mu_B,\omega_B,K_A,j) & ID_A<ID_B\\ H_3(ID_B,\mu_B,\omega_B,ID_A,\mu_A,\omega_A,K_A,j) & ID_A>ID_B\end{cases}$$

2)同理,用户 B 使用相同的算法,进行如下计算:

$$K_B=(\mu_A h_{B,A}\omega_A y^{Q_A})^{h_{A,B}z_B+d_B}$$

然后计算共享密钥:

$$K_{B,A}=\begin{cases}H_3(ID_A,\mu_A,\omega_A,ID_B,\mu_B,\omega_B,K_B,j) & ID_A<ID_B\\ H_3(ID_B,\mu_B,\omega_B,ID_A,\mu_A,\omega_A,K_B,j) & ID_A>ID_B\end{cases}$$

3.3　协议正确性分析

用户 A 拥有自己的私钥 $SK_A(z_A,d_A)$、用户 B

的公钥 $PK_B(\mu_B,\omega_B)$以及系统公共参数。用户 A 计算得出的共享密钥为:

$$\begin{aligned}K_A &= (\mu_B\ h_{A,B}\omega_B y^{Q_B})^{\ h_{B,A}z_A+d_A}\\ &= ((g^{z_B})^{\ h_{A,B}}g^{s_B}(g^s)^{H_1(ID_B,\omega_B,\mu_B)})^{h_{B,A}z_A+d_A}\\ &= (g^{h_{A,B}z_B+s_B+sH_1(ID_B,\omega_B,\mu_B)})^{h_{B,A}z_A+d_A}\\ &= g^{(h_{A,B}z_B+d_B)(h_{B,A}z_A+d_A)}\end{aligned}$$

用户 B 拥有私钥 $SK_B(z_B,d_B)$、用户 A 的公钥 $PK_A(\mu_A,\omega_A)$以及系统公共参数。用户 B 计算得出的共享密钥为:

$$\begin{aligned}K_B &= (\mu_A^{\ h_{B,A}}\omega_A y^{Q_A})^{h_{A,B}z_B+d_B}\\ &= ((g^{z_A})^{\ h_{B,A}}g^{s_A}(g^s)^{H_1(ID_A,\omega_A,\mu_A)})^{h_{A,B}z_B+d_B}\\ &= (g^{h_{B,A}z_A+s_A+sH_1(ID_A,\omega_A,\mu_A)})^{h_{A,B}z_B+d_B}\\ &= g^{(h_{B,A}z_A+d_A)(h_{A,B}z_B+d_B)}\end{aligned}$$

可见,$K_A=K_B$,然后用户 A,B 使用一致的方法生成 K_{AB}和 K_{BA},因此,$K_{AB}=K_{BA}$,满足一致性要求,双方计算出相同的会话密钥。

4 协议安全性及效率分析

4.1 安全性分析

对本文协议进行安全性分析:

(1) 安全模型。本文协议的安全性由挑战者 C 和攻击者 A_I,A_{II}之间的游戏来描述。无证书环境下存在 2 类攻击者:第 1 类攻击者 A_I 表示一个普通的攻击者,他不知道系统主密钥,但是可以替换用户公钥;第 2 类攻击者 A_{II}模拟 KGC 的被动攻击,他知道系统的主密钥,但是不能替换用户的公钥。

(2) 系统建立。挑战者运行 *Setup* 算法,然后将系统参数 *params* 发送给给 A_I,将系统参数 *params* 和系统主密钥 *msk* 发送给 A_{II}。

(3) 询问阶段。敌手可以做如下询问:公钥询问 PublicKeyExtract,部分私钥询问 PartialKeyExtract,秘密值询问 SecretValueExtract,公钥替换 PublicKeyReplace,共享对称密钥询问 SharedKeyReveal。

(4) 猜测阶段。敌手选择 2 个用户 A,B 的共享密钥 K_{AB}。然后随机选择 $b\in\{0,1\}$,如果 $b=0$ 则返回 K_{AB}给敌手;否则随机选取 $K'_{AB}\in\{0,1\}^n$,n 为 K_{AB}的长度,返回 K'_{AB}给敌手。敌手猜测 b',如果 $b'=b$ 则敌手获胜。

如果不存在多项式时间的敌手 A_I,A_{II}能够以不可忽略的优势赢得上述游戏,则称该 NIKE 方案是安全的。

游戏中对敌手 A_I,A_{II}做如下限制:A_I 不能对 (ID_A,ID_B)进行 PartialKeyExtract 询问;A_{II}不能进行 SecretValueExtract 询问和 PublicKeyReplace 询问;敌手 A_I,A_{II}不能对 (ID_A,ID_B)进行 SharedKeyReveal 询问。

定理 1 在随机预言模型下,如果 CDH 难题假设成立,则本文提出的协议是安全的。本定理由以下2 个引理得出。

引理 1 假设 CDH 问题是困难的,本文协议在随机预言模型下对第 1 类攻击者是安全的。详细地,如果存在一个敌手 A_I,能够在多项式时间内以不可忽略的优势赢得上述游戏,则存在一个算法能够以不可忽略的优势解决 CDH 问题。

证明:挑战者 C 收到一个 CDH 问题实例(g,g^a,g^b),C 把 A_I 作为子程序在游戏中与其交互,目标是计算出 g^{ab}。

(1)C 运行 *Setup* 算法,将系统公共参数 *params* 发送给 A_I,随机选择用户 A 和用户 B。

(2)询问阶段:设置用户 A 的部分私钥为 a,用户 B 的部分私钥为 b(a,b 未知)。

1)H_1 询问:维护列表 $L_1(ID,\omega,\mu,e)$,如果询问元组(ID,ω,μ)已经存在则返回 e,否则随机选择 $e\in Z_q^*$,返回 e 并更新列表。

2)PartialKeyExtract(ID)询问:维护列表 $L_{partial}(ID,d)$。如果 $ID\in\{A,B\}$,则 C 退出;否则C 随机选取 z,$s\in Z_q^*$,计算$\mu=g^z$,$\omega=g^s$,$d=s+xH_1(ID,\omega,\mu)\omega=g^s$,返回 d。将条目(ID,d)插入列表 $L_{partial}$,将条目(ID,ω,μ)插入列表 L_{pub},将条目(ID,z)插入列表L_{val}。

3)PublicKeyExtract(ID)询问:维护列表$L_{pub}(ID,\mu,\omega)$,如果 ID 存在于列表中,则查询并返回(μ,ω);否则,如果 $ID\notin\{A,B\}$,首先进行 PartialKeyExtract(ID)询问,然后返回(μ,ω);如果 $ID\in\{A,B\}$,假设 $ID=A$,随机选取 e,$z\in Z_q^*$,计算 $\omega=g^a g^{-xe}$,$\mu=g^z$,将(ID,ω,μ,e)插入 L_1,将(ID,ω,μ)插入 L_{pub},将(ID,z)插入 L_{val}。由于 $\omega y^{Q_{ID}}=g^a g^{-xe}g^{xe}=g^a$,因此这样的模拟是合法的。若 $ID=B$,计算 $\omega=g^b g^{-xe}$,其余操作相同。

4)SecretValueExtract(ID)询问:维护列表 $L_{val}(ID,z)$,如果 ID 存在于列表中则返回 z;否则进行 PublicKeyExtract(ID)询问,然后返回 z。

5)PublicKeyReplace 询问:敌手 A_I 输入要替换公钥的用户 ID 和要替换的公钥,C 查找列表 L_{pub},替换(ID,ω,μ)为 A_I 选择的(ID,μ',ω'),将 L_{val}中条目设置为(ID,z')。

6)SharedKeyReveal(ID_1,ID_2)询问:用户共享密钥询问,如果$(ID_1,ID_2)=(ID_A,ID_B)$,则 C 退出游戏;否则使用 ID_1 的私钥和 ID_2 的公钥(或者 ID_2 的

私钥和ID_1 的公钥)计算并返回 SharedKey 给A_I。

(3)猜测阶段:A_I 选取一对(ID_1,ID_2)进行猜测,如果(ID_1,ID_2)≠(ID_A,ID_B),则 C 退出游戏;否则 C 随机选取 $K_{AB}\in\{0,1\}^n$ 返回给 A_I。如果 A_I 能成功猜出(ID_A,ID_B)的会话密钥,则他必定询问过 $H_3(ID_A,\mu_A,\omega_A,ID_B,\mu_B,\omega_B,K_A,j)$,C 计算如下结果作为 CDH 问题的解答:

$$\frac{K_A}{g^{h_{B,A}z_A\cdot h_{A,B}z_B}\,(g^b)^{h_{B,A}z_A}\,(g^a)^{h_{A,B}z_B}}=g^{ab}$$

根据上述证明,如果 A_I 能够攻破协议,则模拟者可以利用其解决 CDH 问题,而解决 CDH 问题是假设困难的。综上所述,该协议对攻击者 A_I 是安全的。

引理 2　假设 CDH 问题是困难的,本文协议在随机预言模型下对第 2 类攻击者是安全的。详细地,如果存在一个敌手 A_{II}能够在多项式时间内以不可忽略的优势赢得上述游戏,则存在一个算法能够以不可忽略的优势解决 CDH 问题。

证明:挑战者 C 收到一个 CDH 难题实例(g,g^a,g^b),目标是计算出 g^{ab},C 把 A_{II}作为子程序并在游戏中与其交互。C 选择用户 A,B,设置 $\mu_A=g^a$,$\mu_B=g^b$。如果 A_{II}最后获得了游戏的胜利,则 C 计算:

$$\left(\frac{K_A}{(g^a)^{h_{B,A}d_B}\,(g^b)^{h_{A,B}d_A}g^{d_Ad_B}}\right)^{\frac{1}{h_{A,B}h_{B,A}}}=g^{ab}$$

作为 CDH 问题的解答,即如果敌手 A_{II}能够攻破协议,则存在一个算法能够利用 A_{II}解决 CDH 问题,而解决 CDH 问题是假设困难的。综上所述,该协议对攻击者 A_{II}是安全的。

本文协议具有部分前向安全性,如果之前所协商的共享对称密钥不慎泄露,但是双方私钥都处于保密,那么下一次协商出的对称密钥对攻击者来说也是保密的。

4.2　效率分析

4.2.1　通信效率分析

由于本文协议采用非交互式密钥协商的设计思想,因此节省了通信耗时以及发送信号所产生的能量消耗,在传输时延较大的空间 DTN 环境中,本文协议的优势更加明显,与其他协议的比较结果如图 3 所示。其中,横坐标为特殊网络环境中的传输时延;纵坐标表示从发起密钥协商到用户完成计算共享密钥结束所用时间;文献[5-6]协议为交互式密钥交换协议;文献[7]和本文协议为非交互式密钥交换协议。

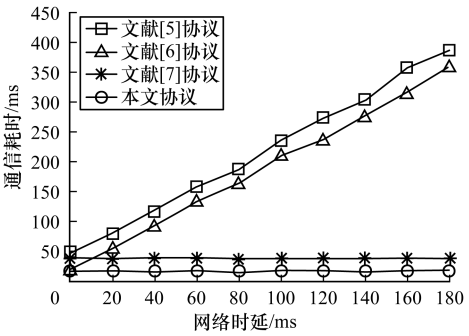

图 3　不同网络时延下各协议通信耗时对比

由图 3 可见,随着网络环境的传输时延增大,交互式密钥交换协议的通信耗时呈线性增长,而非交互式密钥交换协议的通信耗时几乎不变。

4.2.2　计算效率分析

对文献[7,13-14]密钥协商协议进行计算效率分析。在 PIV 3 GHz 处理器、512 MB 内存环境下,各种密码基本单元的计算耗时如表 1 所示。其中,sca. mul 代表标量乘。

表 1　密码基本单元计算耗时　　ms

密码基本单元	耗时
Modular exp	5.31
Pairing	20.04
Pairing-based sca. mul	6.38
ECC-based sca. mul	2.21
Map-to-point hash	3.04

比较单个用户完成密钥协商所需的计算耗时,并采用文献[15]的简单方法评估计算效率。各协议计算耗时对比结果如图 4 所示。其中,纵坐标表示用户计算出共享密钥所需的时间。

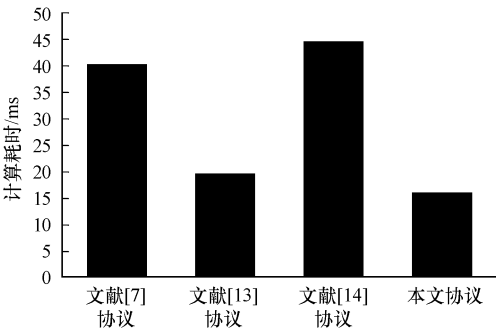

图 4　各协议计算耗时对比

文献[7]协议是基于身份的非交互式密钥交换协议,使用了 2 个双线性对操作;文献[13]协议属于自认证公钥密码(Self-certified PKC),计算共享密钥时使用一个双线性对操作,但是需要使用额外的一个双线性对来验证公钥;文献[14]协议需要使用 2 个双线性对及 2 个点乘操作;而本文协议由于未使

用计算代价最高的双线性对运算,因此在计算效率方面计算代价较低,具有明显优势。同时,由于计算量的大小会直接影响通信终端节点的能量消耗,因此对于计算能力受限的网络终端和能量资源宝贵的网络环境,本文方案优势会更明显。

5 结束语

本文针对空间 DTN 高延时、连接易中断等特点,提出一种适用于空间 DTN 环境的非交互式密钥交换协议。该协议结合无证书密码和非交互式协议的设计思想,无需用户交互,并且可避免证书的使用和密钥托管问题。数据分析结果表明,本文协议较传统协议具有更高的存储、计算和通信效率,更适用于节点能量受限的空间 DTN。本文协议的安全性证明是在随机预言模型下进行的,如何构建标准模型下可证安全且高效的协议,是下一步的研究方向。

参考文献

[1] Lü Xixiang, Mu Yi, Li Hui. Non-interactive Key Establishment for Bundle Security Protocol of Space DTNs[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(1): 5-13.

[2] DTNRG. Bundle Security Protocol Specification[Z]. 2011.

[3] Kate A, Zaverucha G M, Hengartner U. Anonymity and Security in Delay Tolerant Networks[C]//Proceedings of the 3rd International Conference on Security and Privacy in Communications Networks. Washington D. C., USA: IEEE Press, 2007: 504-513.

[4] Jia Zhongtian, Lin Xiaodong, Tan Senghua, et al. Public Key Distribution Scheme for Delay Tolerant Networks Based on Two-channel Cryptography[J]. Journal of Network and Computer Applications, 2012, 35(3): 905-913.

[5] 吴 杨,矫文成,潘艳辉,等. 基于身份的分布式卫星网络私钥管理方案[J]. 计算机科学,2011,38(10):96-99.

[6] Tong D, Liu J W, Mao K F, et al. Certificateless and Pairing-free Key Agreement Scheme for Satellite Network[C]//Proceedings of 2014 Communications Security Conference. [S.l.]: IET, 2014: 1-5.

[7] Dupont R, Enge A. Provably Secure Non-interactive Key Distribution Based on Pairings[J]. Discrete Applied Mathematics, 2006, 154(2): 270-276.

[8] Paterson K G, Srinivasan S. On the Relations Between Non-interactive Key Distribution, Identity-based Encryption and Trapdoor Discrete Log Groups[J]. Designs, Codes and Cryptography, 2009, 52(2): 219-241.

[9] Freire E S V, Hofheinz D, Kiltz E, et al. Non-interactive Key Exchange[C]//Proceedings of the 16th International Conference on Practice and Theory in Public-key Cryptography. Berlin, Germany: Springer-Verlag, 2013: 254-271.

[10] Çapar Ç, Goeckel D, Paterson K G, et al. Signal-flow-based Analysis of Wireless Security Protocols[J]. Information and Computation, 2013, 226: 37-56.

[11] Al-Riyami S S, Paterson K G. Certificateless Public Key Cryptography[M]//Laih C. Advances in Cryptology-ASIACRYPT 2003. Berlin, Germany: Springer-Verlag, 2003: 452-473.

[12] Khabbaz M J, Assi C M, Fawaz W F. Disruption-tolerant Networking: A Comprehensive Survey on Recent Developments and Persisting Challenges[J]. IEEE Communications Surveys & Tutorials, 2012, 14(2): 607-640.

[13] Wu T, Lin H. Non-interactive Authenti-cated Key Agreement over the Mobile Communication Network[J]. Mobile Networks and Applications, 2013, 18(5): 594-599.

[14] 魏 云,魏福山,马传贵. 一种强安全的无证书非交互密钥交换协议[J]. 计算机科学,2014,41(12):101-106.

[15] Cao Xuefei, Kou Weidong, Du Xiaoni. A Pairing-free Identity-based Authenticated Key Agreement Protocol with Minimal Message Exchanges[J]. Information Sciences, 2010, 180(15): 2895-2903.

编辑 金胡考

(上接第 136 页)

[8] 刘 伟,罗 嵘,杨华中. 一种轻量级的无线传感器网络密钥建立协议[J]. 电子与信息学报,2010,32(4):869-873.

[9] 李慧贤,庞辽军,王育民. 适合 Ad Hoc 网络无需安全信道的密钥管理方案[J]. 通信学报,2010,31(1):112-117.

[10] 韩 磊,刘吉强,韩 臻,等. 移动 Ad Hoc 网络预分配非对称密钥管理方案[J]. 通信学报,2012,33(10):26-34.

[11] Ritter H, Winter R, Schiller J. A Partition Detection System for Mobile Ad-hoc Networks[C]//Proceedings of the 1st IEEE International Conference on Sensing. Washington D. C., USA: IEEE Press, 2004: 489-497.

[12] Shamir A. How to Share a Secrete[J]. Communications of the ACM, 1979, 22(11): 612-613.

[13] Simmons G J. How to (Really) Share a Secrete[EB/OL]. (2007-12-16). http://csdl2.computer.arg/.

[14] 葛 蒙,赵曦滨,林国恩. 适用于移动自组织网的鲁棒性密钥管理[J]. 清华大学学报:自然科学版,2008,33(41):1194-1197.

[15] 许俊杰,曾贵华. 基于椭圆曲线的 Ad Hoc 网络门限身份认证方案[J]. 计算机工程与应用,2007,43(17):1045-1048.

编辑 顾逸斐